REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Yours: 12.03.2025 nr

redakcja@omnimodo.com.pl

Ours: 27.03.2025 nr 2.2-9/25/794-2

Answer to request

Estonian Data Protection Inspectorate received your questions regarding the data breach notifications. We will answer your questions accordingly.

1. **What is the purpose – in the light of the GDPR - of notifying the personal data breaches to the supervisory authority? What did the legislator want to achieve through this obligation?**

   Article 33 GDPR states that in case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The purpose of notifying the supervisory authority is to investigate the data breach, decide what measures need to be taken regarding supervisory proceedings and to react as soon as possible to protect the rights and freedoms of data subjects. EDPB has stated that breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data.[1]

2. **Which moment do you consider as "having become aware of the personal data breach". In the opinion of your supervisory authority from which point in time the 72-hour time limit to notify the supervisory authority starts to run?**

   The 72-hour time limit to notify the supervisory authority starts to run as soon as the controller becomes aware that a personal data breach has occurred. The controller is required to take all appropriate technological protection and organisational measures to establish whether a breach has taken place. Therefore, it is an obligation for the controller to detect whether a data breach has occurred. The controller must be considered aware if the controller is certain that a breach of security has occurred that has led to a compromise of personal data.[2]

3. **Should the controller notify to the supervisory authority each personal data breach regardless of the identified level of risk or can it refrain from notifying in case that the assessed risk is at low level?**

   The controller shall notify the supervisory authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons according to the Article 33 (1) GDPR. EDPB has given an example, if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. However, it is important to note, that the risks may have to be re-evaluated if later it becomes evident that a vulnerability in the encryption

[1] European Data Protection Board Guidelines 9/2022 on personal data breach notification under GDPR, Adopted 10 October 2022, page 6.
[2] Ibid, page 11.

software is exposed, then the notification may be required.[3]

4. **Are there any personal data breaches which in view of your supervisory authority should not to be notified to the supervisory authority considering their commonness or specificity - e.g. sending mistakenly an e-mail to the wrong addressee?**

   The controller is required to decide whether to notify us of the data breach or not pursuant to the GDPR. As mentioned above, in some cases it is obligatory to notify us. Mistakenly sent data breach notifications, e.g. from data subjects, will be answered and explained how the letter is categorized moving forward.

5. **How many personal data breaches have been notified to your supervisory authority in the years 2022, 2023 and 2024?**

   Data breach notification statistics:153 notifications in 2022, 196 notifications in 2023 and 184 notifications in 2024.[4]

6. **Which obligations arising from the GDPR concerning handling personal data breach can be fulfilled by the DPO, in particular whether the DPO can assess the personal data breach, notify the breach to the SA, communicate the breach to the data subjects or document the breach internally?**

   According to the Article 38 (1) GDPR the controller and the processor are required to ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The DPO is not personally responsible for ensuring that the controller or the processor is GDPR compliant. The DPO shall inform and advise the controller or processor, monitor compliance with the GDPR and act as a contact point for supervisory authority and data subjects. Pursuant to the Article 33 (5) GDPR the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. Whereas the DPO is required to monitor compliance with the GDPR the DPO may be the one to document the data breaches. Nonetheless, the controller or the processor is the responsible for ensuring the processing of personal data is in compliant with GDPR and that the data breach notification is made to the supervisory authority when needed.

7. **How should the DPO cooperate with the controller in case of personal data breach? What should be the scope of the DPO assistance?**

   The DPO-s task is to inform and advise the controller or processor and monitor the compliance with GDPR. Recital 97 of the GDPR summarises that the DPO is a person with expert level knowledge of data protection law and practices who assists and supervises the data controller in the compliance with the GDPR. Therefore, when any data breach occurs, the DPO-s task is to advise the controller or processor to be compliant with GDPR.

8. **How the DPO should support the controller in handling the personal data breach to avoid risk of the potential conflict of interest? If such a conflict of interest really exists?**

   Pursuant to the Article 38 (6) GDPR the controller or the processor shall ensure that DPO-s other tasks do not create a conflict of interests. The conflict of interests may appear when the DPO-s tasks are carried out by the CEO. Consequently, the DPO has to be independent when carrying out the DPO tasks as stated in the GDPR.

Best regards

Grete-Liis Kalev
lawyer
authorized by Director General

[3] European Data Protection Board Guidelines 9/2022 on personal data breach notification under GDPR, Adopted 10 October 2022, page 18-19.
[4] Estonian Data Protection Inspectorate, statistics (in Estonian) https://www.aki.ee/meist/teadlikkus/statistika